A U F T R A G S V E R A R B E I T U N G S V E R T R A G

abgeschlossen zwischen

1. **Austrian Power Grid AG**
   FN 177696v
   Wagramer Straße 19 (IZD-Tower)
   1220 Wien
   Österreich

   als Verantwortlicher
   im Folgenden kurz „**Auftraggeber**“ genannt, einerseits

und

2. **[Name],** [Firmenbuchnummer], [Adresse]

   als Auftragsverarbeiter
   im Folgenden kurz „**Auftragnehmer**“ genannt, andererseits

   gemeinsam im Folgenden kurz „**Vertragsparteien**“

wie folgt:

1. AUFTRAG

1.1. Der Gegenstand und Umfang dies Auftrages ergibt sich aus [xxx] vom [Datum] (Anlage ./1) (gemeinsam im Folgenden kurz „**Leistungsvereinbarung**“).

2. VERTRAGSDAUER

2.1. Die Laufzeit dieses Auftragsverarbeitungsvertrages ergibt sich aus der Leistungsvereinbarung.

2.2. Dieser Auftragsverarbeitungsvertrag kann von beiden Vertragsparteien mit einer Frist von einem Monat jeweils zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Auflösung aus wichtigem Grund bleibt hiervon unberührt.

3. DATENVERARBEITUNGEN DURCH DEN AUFTRAGNEHMER

3.1. Die Art, der Zweck, der Umfang sowie die Mittel der im Rahmen der Auftragserfüllung notwendigen Verarbeitungen personenbezogener Daten durch den Auftragnehmer sind in der Leistungsvereinbarung beschriebenen.

3.2. Folgende personenbezogene Datenarten werden vom Auftragnehmer zur Auftragserfüllung verarbeitet:

- [Datenarten] zB.: Kontaktdaten, Planungsdaten, Anrainer Grundbuchdaten, etc.

3.3. Die zur Auftragserfüllung notwendigen Verarbeitungen betreffen folgende Betroffenenkategorien:

- [Betroffenenkategorien] zB.: Kunden, Interessenten, Abonnenten, Lieferanten, etc

3.4. Als Kontaktperson für Datenschutzangelegenheiten gibt der Auftragnehmer [Ansprechpartner

& Kontaktdaten] bekannt.

3.5. Der Auftragnehmer hat alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen zu ergreifen, um die Sicherheit der Verarbeitung zu gewährleisten und den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32 DSGVO zu unterstützen.

Der Auftragnehmer hat dem Auftraggeber vor Beginn der Auftragserfüllung das Bestehen folgender Kontrollmaßnahmen in seinem Betrieb zur Überprüfung eines risikoangemessenes Schutzniveaus iSd. Art. 32 DSGVO zu bestätigen:

- Mechanische Schlüssel bzw. Schließsysteme
- Sichere Passwörter, inkl. Mindestlänge sowie techn. oder org. Regelungen zur Komplexität
- Rollen- oder gruppenbasiertes Zugriffskontrollsystem
- Konsequente Umsetzung des Need-to-Know-Prinzips
- Protokollierung der ändernden Benutzerzugriffe (Anlegen, Ändern, Löschen)
- Protokollierung aller Benutzerzugriffe (Lesen, Anlegen, Ändern, Löschen …)
- Mandantenfähigkeit
- Verschlüsselung am Transportweg (VPN-Tunnel, TLS Encryption)
- Protokollierung
- Umfassende, vollständige, regelmäßige Datensicherung
- Automatisch aktualisierter Virenschutz auf sämtlichen IT-Systemen, inkl. Monitoring
- Geprüftes und regelmäßig gewartetes Firewallsystem
- Betrieb eines formalen Incident Response-Management
- Einbindung des IRM in die Meldung und Bearbeitung von Datenschutzverletzungen
- Frühzeitige Einbindung des Datenschutzbeauftragten/-verantwortlichen in die IT-Planung
- Evaluierung aller IT-Vorhaben hinsichtlich der Auswirkungen auf den Datenschutz
- Formalisiertes Auftragsmanagement
- Vorab-Prüfung vor Beauftragung von Dienstleistern
- Einbinden der Datenschutzthematik in die Einschulung neuer Mitarbeiter
- Anbieten von Schulungsmaßnahmen und Veranstaltungen zur Informationssicherheit

- Anbieten von Schulungsmaßnahmen und Veranstaltungen zur Datenschutzthematik
- Verpflichtende Teilnahme an Datenschutz- und Informationssicherheitsschulungen

Der Auftragnehmer verpflichtet sich, dieses dem Auftraggeber gegenüber bekanntgegebene Schutzniveau durch etwaige Änderungen der getroffenen technischen und organisatorischen Maßnahmen nicht zu unterschreiten. Der Auftraggeber darf regelmäßig die vom Auftragnehmer zum Schutz der vom Auftraggeber überlassenen personenbezogenen Daten getroffenen technischen und organisatorischen Maßnahmen kontrollieren, um sicherzustellen, dass diese dem Stand der Technik entsprechen.

4. VERPFLICHTUNGEN DES AUFTRAGNEHMERS UND DES AUFTRAGGEBERS

4.1. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu den im Rahmen des Auftrages vom Auftraggeber überlassenen personenbezogenen Daten sowie daraus resultierenden Verarbeitungsergebnissen hat, dürfen diese Daten ausschließlich entsprechend den Bestimmungen dieses Vertrages sowie allfälligen zusätzlichen schriftlichen Weisungen des Auftraggebers für Zwecke und im Rahmen der Auftragserfüllung verarbeiten, es sei denn, dass sie gesetzlich zur darüber hinausgehenden Verarbeitung verpflichtet sind. In diesem Fall teilt der Auftragsnehmer dem Auftraggeber diese gesetzlichen Verpflichtungen bzw. Anforderungen vor der Verarbeitung mit, sofern nicht eine solche Mitteilung gesetzlich untersagt ist.

Die überlassenen Daten dürfen vom Auftragnehmer und jeder ihm unterstellten Person, die Zugang zu diesen Daten hat, ausschließlich dem Auftraggeber zurückgegeben oder nur nach dessen schriftlicher Weisung an Dritte übermittelt werden. Eine Verwendung der vom Auftraggeber überlassenen personenbezogenen Daten für eigene auftragsfremde Zwecke durch den Auftragnehmer ist nicht zulässig.

4.2. Der Auftragnehmer ist verpflichtet, unterstützend mitzuwirken, dass der Auftraggeber die ihm obliegenden gesetzlichen Pflichten zur Auskunftserteilung, zur Berichtigung und Löschung, zur

Einschränkung der Verarbeitung sowie zur Übertragung gegenüber den von der Datenverarbeitung betroffenen Personen innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und stellt dem Auftraggeber auf Anfrage unverzüglich alle hierzu notwendigen Informationen zur Verfügung. Eine eigenmächtige Auskunftserteilung, Berichtigung oder Löschung, Einschränkung der Verarbeitung oder Übertragung der im Rahmen des Auftrages vom Auftraggeber überlassenen personenbezogenen Daten durch den Auftragnehmer ist nicht zulässig und darf nur nach schriftlicher Weisung des Auftraggebers erfolgen. Soweit sich eine betroffene Person unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.3. Der Auftragnehmer verpflichtet sich, den Auftraggeber – soweit gesetzlich zulässig – unverzüglich über Maßnahmen der Datenschutzbehörde, welche den Auftrag betreffen, zu informieren. Weiters verpflichtet sich der Auftragnehmer, den Auftraggeber in Verfahren aller Art, welche mit der Auftragserfüllung im Zusammenhang stehen, zu unterstützen.

4.4. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei Feststellung von Verletzungen des Schutzes personenbezogener Daten („Datenpannen“) im Sinne der Art. 33 und 34 DSGVO unverzüglich zu informieren und diesem die in Art. 33 Abs. 3 DSGVO genannten Informationen zur Verfügung zu stellen. Der Auftragnehmer hat den Auftraggeber auch bei der Erfüllung der Meldepflichten iSd. Art 33 und 34 DSGVO, bei der Vornahme von Datenschutz-Folgenabschätzungen sowie bei der Durchführung vorheriger Konsultationen im Sinne des Art. 36 DSGVO zu unterstützen.

4.5. Der Auftragnehmer wird ohne schriftliche Genehmigung des Auftraggebers keine Kopien der im Rahmen des Auftrages vom Auftraggeber überlassenen personenbezogenen Daten erstellen. Hiervon ausgenommen sind Sicherheitskopien, welche zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.

5. GEWÄHRLEISTUNGSZUSAGEN DES AUFTRAGNEHMERS

5.1. Der Auftragnehmer wird alle mit der zur Auftragserfüllung notwendigen Datenverarbeitung befassten Personen vor Aufnahme ihrer Tätigkeit zur Wahrung der Vertraulichkeit und des

Datengeheimnisses verpflichten sowie dazu, dass diese Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht bleibt.

5.2. Der Auftragnehmer leistet Gewähr, dass die Erbringung der zur Auftragserfüllung notwendigen Datenverarbeitung ausschließlich in der EU oder dem EWR stattfindet.

5.3. Eine Datenverarbeitung in einem Drittland darf nur nach vorheriger schriftlicher Genehmigung des Auftraggebers erfolgen und nur, soweit dabei zur Wahrung eines angemessenen Datenschutzniveaus die Voraussetzungen der Art. 44 ff. DSGVO erfüllt werden. Das angemessene Datenschutzniveau ergibt sich dabei aus:

- einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO;
- einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO;
- verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO;
- Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO;
- genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO;
- einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO;
- von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO;
- einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

6. SUB-AUFTRAGNEHMER

6.1. Der Auftragnehmer darf Sub-Auftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger schriftlicher Genehmigung des Auftraggebers beauftragen. Dieses Genehmigungserfordernis gilt auch für den Wechsel eines Sub-Auftragnehmers.

6.2. Der Auftragnehmer hat mit einem vom Auftraggeber im Sinne des Punktes 6.1. genehmigten Sub-Auftragnehmer einen schriftlichen Sub-Auftragsverarbeitungsvertrag im Sinne des Art. 28 Abs. 4 DSGVO abschließen, in welchem durch entsprechende Gewährleistungen des Sub-

Auftragnehmers sicherzustellen ist, dass dem Sub-Auftragsnehmer dieselben datenschutzrechtlichen Verpflichtungen (insbesondere technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten) obliegen, an die auch der Auftragsnehmer aufgrund des Gesetzes sowie aufgrund dieser Vereinbarung gebunden ist. Der Auftraggeber ist jederzeit berechtigt, Einsicht in die schriftlichen Sub-Auftragsverarbeitungsverträge zu nehmen bzw. diesen vor Genehmigung eines Sub-Auftragsverarbeiters zu prüfen. Erbringt der Sub-Auftragnehmer seine Leistung außerhalb der EU bzw. des EWR, so hat der Auftragnehmer die datenschutzrechtliche Zulässigkeit der vom Sub-Auftragnehmer vorzunehmenden Datenverarbeitungen durch entsprechende Gewährleistungszusagen durch den Sub-Auftragnehmer sicherzustellen.

6.3. Die Weitergabe von personenbezogenen Daten an den Sub-Auftragnehmer und dessen erstmaliges Tätigwerden sind erst nach Abschluss des Sub-Auftragsverarbeitungsvertrages gestattet.

7. WEISUNGS- UND KONTROLLRECHTE DES AUFTRAGGEBERS

7.1. Der Auftraggeber ist berechtigt, dem Auftragnehmer jederzeit in schriftlicher Form Weisungen im Zusammenhang mit den zur Auftragserfüllung notwendigen Datenverarbeitungen zu erteilen.

7.2. Wenn er der Ansicht ist, dass eine Weisung im Sinne des Punktes 7.1. gesetzeswidrig sei, ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich darüber in Kenntnis zu setzen.

7.3. Der Auftraggeber hat im Zusammenhang mit der Verarbeitung der von ihm im Rahmen des Auftrages überlassenen personenbezogenen Daten das Recht auf jederzeitige Kontrolle der Einhaltung der Pflichten des Auftragnehmers im Sinne des Art. 28 DSGVO sowie dieses Vertrages. Der Auftragnehmer hat dem Auftraggeber dabei jene Informationen zur Verfügung zu stellen sowie insoweit Zugang zu seinen Datenverarbeitungseinrichtungen zu gewähren und den Auftraggeber sonst soweit zu unterstützen, wie dies zu einer wirksamen Kontrolle – unter Wahrung des Datenschutzes gegenüber Dritten – notwendig ist.

8. LÖSCHUNG DER DATEN

8.1. Mit Beendigung des Auftrages hat der Auftragnehmer sämtliche im Rahmen des Auftrages vom Auftraggeber überlassenen personenbezogenen Daten sowie daraus resultierende Verarbeitungsergebnisse (inkl. Sicherheitskopien) dem Auftraggeber zu übergeben oder nach vorheriger schriftlicher Weisung des Auftraggebers datenschutzgerecht zu vernichten, soweit und solange nicht aufgrund anwendbarer rechtlicher Bestimmungen eine Verpflichtung zur Speicherung dieser Daten besteht.

9. SCHLUSSBESTIMMUNGEN

9.1. Änderungen oder Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses bzw. das Abgehen davon.

9.2. Dieser Vertrag unterliegt österreichischem Recht unter Ausschluss der Verweisungsnormen des Internationalen Privatrechts sowie des UN-Kaufrechts.

9.3. Gerichtsstand ist der Geschäftssitz des Auftraggebers.

9.4. Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam sein oder werden, so wird jedoch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die Vertragsparteien verpflichten sich für diesen Fall, anstelle von ungültigen Vereinbarungen solche gültigen zu treffen, welche dem Sinn und wirtschaftlichem Zweck dieses Vertrages am nächsten kommen.

10. ZERTIFIZIERUNGEN

Folgende gültige Zertifizierungen anhand einschlägiger Normen aus dem Informationssicherheitsbereich (z.B. ISO 27000-Familie u.ä.) liegen vor:

Zertifikat	Aussteller	Datum

ANLAGEN

[xxx] vom [Datum] (Anlage ./1)

[Ort], am [Datum]

…… ……

[Auftraggeber] [Auftragnehmer]